United Nations E/CN.15/2018/12

Economic and Social Council

Distr.: General
13 April 2018

Original: English

Commission on Crime Prevention and Criminal Justice
Twenty-seventh session
Vienna, 14–18 May 2018
Item 8 of the provisional agenda*
World crime trends and emerging issues and responses in the field of crime prevention and criminal justice

Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 3 to 5 April 2018

I. Introduction

1. In its resolution 65/230, the General Assembly requested the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, an open-ended intergovernmental expert group, to be convened prior to the twentieth session of the Commission, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

2. The first meeting of the Expert Group was held in Vienna from 17 to 21 January 2011. At that meeting, the Expert Group reviewed and adopted a collection of topics and a methodology for the study (E/CN.15/2011/19, annexes I and II).

3. The second meeting of the Expert Group was held from 25 to 28 February 2013. At that meeting, the Expert Group took note of the draft comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, as prepared by the United Nations Office on Drugs and Crime (UNODC) with the guidance of the Expert Group, pursuant to the mandate contained in General Assembly resolution 65/230, and the collection of topics for consideration within a comprehensive study of the impact of and response to cybercrime and the methodology for that study, as adopted at the first meeting of the Expert Group.

* E/CN.15/2018/1

V.18-02315 (E) 090518 100518

Please recycle

4. In the Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation, adopted by the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice and endorsed by the General Assembly in its resolution 70/174, Member States noted the activities of the Expert Group, the international community and the private sector, and invited the Commission to consider recommending that the Expert Group continue, based on its work, to exchange information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing responses and to propose new national and international legal or other responses to cybercrime.

5. The third meeting of the Expert Group was held from 10 to 13 April 2017. At that meeting, the Expert Group adopted the summaries by the Rapporteur of deliberations at the first and second meetings of the Expert Group and considered, inter alia, a draft comprehensive study of the problem of cybercrime and comments thereto, and the way forward based on the draft study, and exchanged information on national legislation, best practices, technical assistance and international cooperation.

6. In its resolution 26/4, adopted at its twenty-sixth session in May 2017, the Commission on Crime Prevention and Criminal Justice requested the Expert Group to continue its work and, in so doing, to hold periodic meetings and function as the platform for further discussion on substantive issues concerning cybercrime, keeping pace with its evolving trends, and in line with the Salvador Declaration and the Doha Declaration, and requested the Expert Group to continue to exchange information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing responses and propose new national and international legal or other responses to cybercrime.

7. The dates for the fourth meeting of the Expert Group, were decided by the extended Bureau by silence procedure on 23 January 2018, and confirmed at its meeting on 26 January 2018.

II. List of preliminary recommendations and conclusions

8. In line with the workplan of the Expert Group for the period 2018–2021, adopted by the Expert Group at its 1st meeting, on 3 April 2018, the Rapporteur will prepare, at each of the meetings of the Expert Group in 2018, 2019 and 2020, with assistance from the Secretariat and based on the discussions and deliberations of the Expert Group, a list of preliminary conclusions and recommendations suggested by Member States that should be precise and should focus on strengthening practical responses to cybercrime. As specified in the workplan, that list will be included in the report of each meeting in the form of a compilation of suggestions made by Member States, to be discussed further at the stock-taking meeting to be held no later than 2021. Also in accordance with the workplan, at that stock-taking meeting, the Expert Group will consider the preliminary conclusions and recommendations thus collected in order to produce a consolidated and comprehensive list of adopted conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice.

A. Legislation and frameworks

9. In line with the workplan, the present paragraph contains a compilation of suggestions made by Member States at the meeting under agenda item 2 entitled "Legislation and frameworks". These preliminary recommendations and conclusions were submitted by Member States and their inclusion does not imply their endorsement by the Expert Group:

(a) Member States should ensure that their legislative provisions withstand the test of time with regard to future developments in technology by enacting laws with formulations that are technologically neutral and criminalize the activity deemed illegal instead of the means used. Member States should also consider establishing consistent terminology to describe cybercrime activities and facilitate, to the extent possible, accurate interpretations of relevant laws by law enforcement agencies and the judiciary;

(b) Member States should respect the sovereign rights of other States in formulating policies and legislation that meet their national conditions and needs in addressing cybercrime. To foster international cooperation to combat cybercrime, the principle of national sovereignty should not mistakenly be interpreted as an obstacle, but rather be considered fundamental and regarded as a starting point. The volatile nature of electronic data transmission and storage, such as in so-called clouds, may require engaging in multilateral discussions on innovative and expanded mutual assistance between States to ensure timely access to electronic data and evidence;

(c) To prevent and/or eliminate safe havens for criminals, Member States should cooperate with each other to the widest extent possible in investigations, evidence collection, prosecution, adjudication and, where necessary, the removal of illegal content from the Internet. Member States should also offer the greatest degree of flexibility possible in their international cooperation to combat cybercrime and other crimes involving electronic data, either when leading investigations or when sharing evidence, irrespective of whether the underlying activities are denominated differently in the respective States. In doing so, Member States should bear in mind that dual criminality is usually required for extradition but not necessarily for mutual legal assistance;

(d) In formulating policies and legislation, Member States should consider the need to strike a balance between human rights protection on the one hand, and national security, public order and the legitimate rights of third persons on the other. National legislations that criminalize conduct associated with cybercrime and grant procedural authority to investigate, prosecute and adjudicate on cybercrime cases should be consistent with due process guarantees, privacy interests, civil liberties and human rights. National policies and legislations as well as existing and/or future international instruments should follow a multidimensional approach. On the one hand, they should include adequate cybercrime policies based on a comprehensive understanding of the broader concept of cybersecurity. On the other hand, they should not only cover illegal conduct, but also focus on crime prevention and provide help to victims of crime and assistance to the general public. In order to create a solid base for international cooperation on combating cybercrime, Member States should strive to find and promote a culture of establishing a common future for cyberspace;

(e) Member States should pursue international cooperation without requiring full harmonization of national legislation, provided that the underlying conduct is criminalized and laws are sufficiently compatible to simplify and expedite the various forms of such cooperation;

(f) Member States should take into account that domestic legal frameworks continue to have a decisive function in ensuring the effectiveness and overall balance of the system of investigation and prosecution, because criminal law is particularly sensitive in regard to fundamental rights and because investigations in the area of computer crimes concern, to a large extent, the private communications and data of citizens;

(g) To enable the prosecution of criminal acts, Member States should legislate on extraterritorial jurisdiction over citizens and persons ordinarily resident on their territory, irrespective of where those acts were committed and whether they constitute offences in the foreign jurisdiction;

(h) Member States may draw on different legal bases for international cooperation, including reciprocity, bilateral or multilateral treaties and other arrangements. Moreover, Member States with more advanced capacities and infrastructure in the field of cybercrime should assume responsibilities proportionate to those capacities or infrastructure in providing legal assistance to other States;

(i) To ensure that relevant issues are properly considered, Member States should consult all relevant stakeholders, including intergovernmental stakeholders, the private sector and civil society, as early as possible when the decision is made to introduce cybercrime legislation;

(j) Member States should foster strong and trustworthy public-private cooperation in the field of cybercrime, including cooperation between law enforcement authorities and communication service providers. Engaging in a dialogue with private industry, accompanied by public-private partnerships where possible and memorandums of understanding where needed, is also required to strengthen and facilitate cooperation;

(k) Member States should support UNODC in establishing an educational project or programme that focuses on raising awareness of cybercrime and appropriate responses to it among judicial and prosecution authorities, digital forensic experts of Member States and among private entities, and use capacity-building tools or an electronic knowledge management platform to raise awareness of the impact of cybercrime among civil society;

(l) Effective development, enactment and implementation of national legislation to counter cybercrime should be backed up by capacity-building measures and technical assistance programmes. Member States should allocate appropriate resources for domestic capacity-building. The proper implementation of cybercrime-related legislation requires the training of police and prosecutors, as well as public awareness campaigns. Such resources will also further international cooperation, as such cooperation is enhanced by a country's domestic capacity to investigate and prosecute cybercrime-related offences;

(m) Member States should strengthen existing frameworks and networks for combating cybercrime by identifying and addressing the weak points of those frameworks and networks and providing them with the necessary resources so as to improve their effectiveness;

(n) UNODC should engage actively in capacity-building for all Member States in need of assistance, in particular developing countries. Such capacity-building activities should be politically neutral and free from conditions, should result from thorough consultations and be voluntarily accepted by the recipient countries. In terms of substance, those capacity-building activities should cover at least the following areas:

(i) Training for judges, prosecutors, investigators and law enforcement authorities in cybercrime investigations, the handling of electronic evidence, chain of custody and forensic analysis;

(ii) Drafting, amending and/or implementing legislation on cybercrime and electronic evidence;

(iii) Structuring cybercrime investigation units and providing guidance on related procedures;

(iv) Drafting, updating, and implementing legislation to combat the use of the Internet for terrorist purposes;

(o) UNODC should seek synergies and cooperate closely with other stakeholders or organizations such as the Council of Europe and the Organization of American States (OAS) in the field of capacity-building programmes on combating cybercrime to ensure that activities and initiatives in this area are not dispersed or fragmented;

(p) Member States should continue to use the Expert Group as a platform for the exchange of information and best practices, including model laws or model clauses, relating to such issues as jurisdiction, special investigative techniques, electronic evidence, including challenges posed by the volatile nature of electronic evidence and its admissibility in court, and international cooperation;

(q) To avoid fragmentation, Member States should explore universally accepted practices and rules through multilateral consultation under the auspices of the United Nations and through the Expert Group platform;

(r) Member States should evaluate the possibility and feasibility of mandating the Expert Group or UNODC to conduct and make available on a regular basis, with substantive contributions by Member States, an assessment of cybercrime trends;

(s) Member States should develop a new international legal instrument on cybercrime within the framework of the United Nations that takes into account the concerns and interests of all Member States;

(t) Member States should use and/or join existing multilateral legal instruments on cybercrime such as the Council of Europe Convention on Cybercrime (Budapest Convention), as they are considered by many States to be best practice models guiding appropriate domestic and international responses to cybercrime;

(u) Existing legal instruments and mechanisms, including the United Nations Convention against Transnational Organized Crime, should be taken advantage of by as many States as possible to strengthen international cooperation;

(v) Under the auspices of the Expert Group, Member States should explore internationally applicable responses that could be reflected in model laws or model clauses where appropriate, and in doing so should draw on best practices in existing regional instruments and/or national legislation.

B. Criminalization

10. In line with the workplan, the present paragraph contains a compilation of suggestions made by Member States at the meeting under agenda item 3 entitled "Criminalization". These preliminary recommendations and conclusions were submitted by Member States and their inclusion does not imply their endorsement by the Expert Group:

(a) Member States should take into account that many substantive criminal law provisions designed for "offline" crime may also be applicable to crimes committed online. Therefore, to strengthen law enforcement, Member States should use existing provisions in domestic and international law, as appropriate, to tackle crimes in the online environment;

(b) Member States should adopt and apply domestic legislation to criminalize cybercrime conduct and to grant law enforcement authorities procedural authority to investigate alleged crimes consistent with due process guarantees, privacy interests, civil liberties and human rights;

(c) Member States should continue to enact cyber-specific criminal legislation that takes into account new criminal conduct associated with the misuse of information and communications technology to avoid relying on generally applicable provisions of criminal law;

(d) Member States should criminalize core cybercrime offences that affect the confidentiality, integrity and availability of computer networks and computer data, taking into account widely recognized international standards;

(e) Cyber-related acts that are minor infringements rather than criminal offences should be addressed by civil and administrative regulations as opposed to criminal legislation;

(f) To the extent that they have not done so already, Member States should consider the criminalization of:

(i) New and emerging forms of cybercrime activities such as the criminal misuse of cryptocurrencies, offences committed on the darknet and the Internet of things, phishing, and the distribution of malware and any other software used for committing criminal acts;

(ii) The disclosure of personal information and "revenge porn";

(iii) The use of the Internet to commit acts related to terrorism;

(iv) The use of the Internet to incite hate crime and violent extremism;

(v) The provision of technical support to or assistance in the perpetration of an act of cybercrime;

(vi) The establishment of illicit online platforms or the publication of information to perpetrate cyber-related crimes;

(vii) Illegally gaining access to or hacking into computer systems;

(viii) Illegally intercepting or damaging computer data and damaging computer systems;

(ix) Illegally interfering with computer data and systems;

(x) Misuse of devices;

(xi) Computer-related forgery and fraud;

(xii) Child sexual abuse and exploitation;

(xiii) The infringement of copyrights;

(xiv) Child sexual abuse and exploitation, and incitement of minors to commit suicide;

(xv) Unlawfully influencing critical information infrastructure;

(g) Member States should ensure that computer-specific offences are drafted as tailor-made provisions that do not simply extend the application of traditional offences to the digital environment, but take into account the special features of the digital environment and the actual need for criminalization based on a careful assessment;

(h) Member States should bear in mind that the focus of international harmonization concerning criminalization of cybercrime should be on a core set of offences against the confidentiality, integrity and accessibility of information systems, while a need to harmonize criminalization concerning general offences that are committed using information and communications technology should mainly be dealt with in specialized forums concerning specific areas of crime;

(i) Member States should avoid criminalizing a broad range of activities by Internet service providers (ISPs), especially where such regulations may improperly limit legitimate speech and the expression of ideas and beliefs. Member States should instead work with ISPs and the private sector to strengthen cooperation with law enforcement authorities, noting in particular that most ISPs have a vested interest in ensuring that their platforms are not abused by criminal actors;

(j) Member States should adopt and implement domestic legal evidence frameworks to permit the admission of electronic evidence in criminal investigations and prosecutions, including the appropriate sharing of electronic evidence with foreign law enforcement partners;

(k) Member States should use the Organized Crime Convention to facilitate the sharing of information and evidence for criminal investigations relating to cybercrime, given the frequent involvement of organized crime groups in cybercrime;

(l) Member States should explore ways to help to ensure that the exchange of information among investigators and prosecutors handling cybercrime is made in a timely and secure way, including by strengthening networks of national institutions that may be available 24/7;

(m) On the issue of criminalizing ISP non-compliance with law enforcement, Member States should exercise caution and pay meticulous attention to the detrimental effects on private sector activities and fundamental human rights, in particular freedom of speech;

(n) In effectively addressing cybercrime, Member States should take into consideration existing human rights frameworks, in particular as regards freedom of expression and the right to privacy, and should uphold the principles of legality, necessity and proportionality in criminal proceedings relating to the fight against cybercrime;

(o) Member States should identify trends in the activities underlying cybercrime through research and should further evaluate the possibility and feasibility of mandating the Expert Group or UNODC to conduct and make available on an annual basis, with substantive contributions by Member States, an assessment of cybercrime trends;

(p) Member States should consider the adoption of comprehensive strategies against cybercrime that include developing victimization surveys and informing and empowering potential victims of cybercrime;

(q) Member States should consider taking further preventive measures against cybercrime including, but not limited to, measures for the responsible use of the Internet, especially by children and young people.

III. Summary of deliberations

A. Adoption of the Chair's proposal for the workplan of the Expert Group for the period 2018–2021

11. At its 1st meeting, on 3 April 2018, the Expert Group considered agenda item 1 (c), entitled "Adoption of the Chair's proposal for the workplan of the Expert Group for the period 2018–2021". The Chair's proposal for the workplan of the Expert Group for the period 2018–2021 was adopted.

B. Legislation and frameworks

12. At its 2nd, 3rd and 4th meetings, on 3 and 4 April 2018, the Expert Group considered agenda item 2, entitled "Legislation and frameworks".

13. The discussion was facilitated by the following panellists: Lu Chuanying (China); George Maria Iyendezwa (Nigeria); Cristina Schulman (Romania); Pedro Verdelho (Portugal); Claudio Peguero (Dominican Republic); Maria Alejandra Daglio (Argentina); and Mohamed Mghari (Morocco).

14. During the subsequent debate, many delegations referred to legislative and policy developments in their countries to address issues related to cybercrime and cybersecurity. They emphasized the key role of capacity-building and technical

assistance programmes in supporting the successful implementation of national legislation and the building of national capacities for investigation, prosecution and adjudication, and international cooperation. The need for multidisciplinary approaches involving civil society and the private sector was also highlighted.

15. A number of speakers were of the opinion that a new global comprehensive legal instrument on cybercrime was not needed, as they considered already existing international instruments such as the Budapest Convention and the Organized Crime Convention sufficient for developing appropriate domestic and international cooperation responses to cybercrime. According to those speakers, the Budapest Convention provided States parties (which included a number of non-members of the Council of Europe) and States that used the Convention as a reference with an effective legal and operational framework for addressing cross-border cybercrime because, inter alia, it facilitated international cooperation and the harmonization of pertinent criminal law and criminal procedure provisions. Reference was also made to the work of the Cybercrime Convention Committee and the capacity-building projects of the Council of Europe in support of the implementation of the Convention, such as Global Action on Cybercrime Extended, and other outreach projects involving technical assistance, for instance within OAS and the Economic Community of West African States. Moreover, it was stated that negotiations for a new treaty would take up too much time and resources owing to the lack of consensus on crucial aspects such as scope, national sovereignty and jurisdiction, could have an impact on the adoption by States of adequate standards to fight cybercrime.

16. Other speakers reiterated their opinion that new responses were needed, including a new universal or global legal instrument on cybercrime within the framework of the United Nations, to address challenges posed by the fast development of Internet technology that were not covered by existing mechanisms. The view was expressed that existing mechanisms should not prevent international discussions of new responses. Some speakers viewed the Budapest Convention as a regional legal instrument that did not address the concerns of all Member States. Some speakers expressed their concern at the closed nature of the accession process, in that accession was by invitation only and subject to the approval of the States parties. One speaker suggested that one effective legal possibility for cooperation among States that were not parties to the Budapest Convention was the draft United Nations convention on cooperation in combating cybercrime submitted to the Secretary-General on 11 October 2017 (A/C.3/72/12, annex).

17. Several speakers recalled that any instrument had to include proper rules and safeguards to protect basic human rights.

18. Some speakers were of the opinion that the Budapest Convention, in particular its article 32, paragraph (b), presented challenges to international law that were difficult to accept, such as respect for national sovereignty. Other speakers noted that the scope of article 32, paragraph (b), was limited and that some States currently went beyond the provisions of article 32, paragraph (b) without the procedural protections that applied to all articles of the Budapest Convention.

19. As cybercrime was becoming more and more transnational in nature and, in many cases, was related to organized crime, some speakers considered the Organized Crime Convention relevant to fighting cybercrime.

20. The Expert Group also discussed how cybersecurity and cybercrime were related and what were the differences between them. Several speakers indicated that the two were different concepts within the very broad range of challenges that the use of modern information and communications technology presented and that they should therefore be discussed in different and more appropriate forums within the United Nations, such as the International Telecommunication Union or the Group of Governmental Experts on Information Security. Several speakers noted nonetheless that the topics were interlinked as, in practice, issues related to cybersecurity needed to be addressed to effectively counter cybercrime. A plea was made for close cooperation and agreements with the private sector.

21. Many speakers expressed appreciation for the work of UNODC through the Global Programme on Cybercrime and shared examples of technical assistance and capacity-building activities carried out under the programme in their countries or regions. Several speakers also noted that other intergovernmental organizations in their regions, such as the Commonwealth of Independent States, OAS, the African Union, the Shanghai Cooperation Organization and the Council of Europe, were also providing legislative and other types of assistance to counter cybercrime.

22. Speakers expressed appreciation for the work done by the Chair and the Bureau of the Expert Group and by the Secretariat to organize the meeting. Many speakers expressed support for the work of the Expert Group. Some speakers stated that it provided a valuable forum for multilateral discussions among experts from diverse jurisdictions. According to some speakers, the Expert Group could be effective in discussing responses to the common threats posed by cybercrime, including meeting the technical assistance and capacity-building needs of countries. The adoption by the Expert Group of its workplan for the period 2018–2021 was welcomed as a step in the right direction.

23. At its 3rd meeting, the Expert Group continued its consideration of agenda item 2. Speakers raised additional points, in particular the importance of ensuring that the human rights safeguards enshrined in international law and international standards were observed in legislation related to cybercrime and in international cooperation agreements or arrangements, especially those involving electronic evidence. In particular, the importance of balancing the rights to privacy and freedom of expression with the need to prevent and combat cybercrime was discussed. Several speakers observed a higher degree of convergence among jurisdictions in the criminalization of offences related to cybercrime, which helped to decrease the fragmentation of legal norms in this field. Remaining challenges were the further strengthening of international cooperation efforts through both formal and informal cooperation practices, and jurisdictional issues raised by cloud computing.

24. The Expert Group further discussed trans-border access to data. The view was expressed that deliberations on this matter within the Expert Group and in other relevant intergovernmental forums had been very useful in identifying best practices and enhancing cooperation among jurisdictions in the investigation of cybercrime. Respect for the principle of national sovereignty was an issue that needed to be considered further, as it was not always clear how practices in accessing data located in other jurisdictions were compatible with this principle. The proportionality principle in efforts to curb cybercrime was also highlighted. According to many speakers, legislation to counter cybercrime needed to use technologically neutral language in order to keep up with the pace of development in technology and in crime patterns, but should also be specific enough to capture the main criminal activities. Several speakers highlighted the need to address and respond to the increasing use of the Internet for terrorist purposes and to spread hate speech and "fake news" by creating or updating national legislation. The implementation of any legal framework was perceived to be more effective when accompanied by technical assistance and capacity-building projects.

C. Criminalization

25. At its 4th and 5th meetings, on 4 and 5 April 2018, the Expert Group considered agenda item 3, entitled "Criminalization".

26. The discussion was facilitated by the following panellists: Malini Govender (South Africa); Li Jingjing (China); Vadim Sushchik (Russian Federation); Eric do Val Lacerda Sogocio (Brazil); Marouane Hejjouji (Morocco) and Normand Wong (Canada).

27. Many speakers provided information on the ways in which cybercrime was criminalized in their countries. The most common offences mentioned by speakers included cyber-specific offences, often referred to as core cybercrime offences, such

as those targeting the confidentiality, integrity and accessibility of computer systems, as well as cyber-enabled offences, including offences related to child abuse and exploitation, privacy-related offences, offences related to personal data and the use of the Internet for terrorist purposes. Speakers noted that most countries already had legislation that criminalized the core cybercrime offences. Speakers noted that, in order to comply with the principle of dual criminality and to eliminate safe havens for criminals, it was not necessary for States to have the same crime typology, provided that the underlying conduct constituted offences in all jurisdictions.

28. Speakers also emphasized that legislation on the admissibility of electronic evidence in criminal investigations and prosecutions was needed to effectively counter cybercrime. The introduction of such legislation should be accompanied by adequate training and capacity-building for law enforcement officials, prosecutors and judges. The importance of sharing electronic evidence among jurisdictions was also underscored.

29. Speakers shared the experience of their countries in devising legislation and laws to criminalize cybercrime activities. Experts spoke about when it was necessary to create new, specific legislation to criminalize certain acts and when existing legislation and general offences were adequate and sufficient to combat new and emerging forms of cybercrime. Many speakers found it very useful to keep legislation technology-neutral so that it would remain applicable in the face of evolving forms of information and communications technology and cybercrime. Every country had different needs and could consider whether it needed to create new offences depending on the crime trends it faced. Speakers also noted the necessity of having adequate legislation to criminalize new and emerging forms of crime fuelled by the criminal misuse of, inter alia, cryptocurrencies, the Internet of things and the darknet.

30. The Expert Group discussed issues related to sanctions for ISPs that failed to cooperate with law enforcement or that failed to comply with legal requirements relating to the prevention of cybercrime. The Expert Group also discussed how the private sector could cooperate with law enforcement based on identified best practices relating to the legal responsibilities and the accountability of ISPs. Other speakers noted that, at the same time, it was important to take into account human rights safeguards when requiring compliance from ISPs. The question was raised whether the responsibility of ISPs should fall within the scope of criminalization measures.

31. On the subject of preventing cybercrime, several speakers emphasized the importance of developing awareness-raising campaigns for the general public as well as targeted education programmes for children in order to inform them about the risks of cybercrime and improve online safety and cybersecurity for the country as a whole. Moreover, tailored training courses and appropriate allocation of resources were needed in order to enhance the capacities of law enforcement to prevent cybercrime activities.

IV. Organization of the meeting

A. Opening of the meeting

32. The meeting was opened by André Rypl (Brazil), Vice-President of the Expert Group, in his role as Chair of the fourth meeting of the Expert Group.

B. Statements

33. Statements were made by experts of the following States: Albania, Algeria, Argentina, Australia, Belarus, Bosnia and Herzegovina, Brazil, Bulgaria, Canada, Chile, China, Colombia, Costa Rica, Czechia, Dominican Republic, Ecuador, Egypt, El Salvador, Estonia, Georgia, Germany, Ghana, Guatemala, India, Indonesia, Iran (Islamic Republic of), Italy, Japan, Jordan, Kazakhstan, Kuwait, Liechtenstein,

Malaysia, Mauritius, Mexico, Montenegro, Netherlands, Nigeria, Norway, Paraguay, Philippines, Portugal, Republic of Moldova, Romania, Russian Federation, Serbia, South Africa, Sri Lanka, Thailand, the former Yugoslav Republic of Macedonia, Tunisia, Turkey, Ukraine, United Kingdom of Great Britain and Northern Ireland, United States of America and Viet Nam.

34. Statements were also made by representatives of the following intergovernmental organizations: Council of Europe, European Union and Shanghai Cooperation Organization.

C. Adoption of the agenda and other organizational matters

35. At its 1st meeting, on 3 April 2018, the Expert Group adopted the following provisional agenda:

1. Organizational matters:
   (a) Opening of the meeting;
   (b) Adoption of the agenda;
   (c) Adoption of the Chair's proposal for the workplan of the Expert Group for the period 2018–2021.
2. Legislation and frameworks.
3. Criminalization.
4. Other matters.
5. Adoption of the report.

D. Attendance

36. The meeting was attended by representatives of 98 Member States, an observer State, a United Nations Secretariat unit, 4 intergovernmental organizations and 9 institutions representing academia and the private sector.

37. A provisional list of participants was circulated at the meeting (UNODC/CCPCJ/EG.4/2018/NL.1).

E. Documentation

38. The Expert Group had before it, in addition to the draft comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, the following documents:

(a) Provisional agenda (UNODC/CCPCJ/EG.4/2018/1);

(b) Proposal by the Chair for the 2018–2021 workplan of the Expert Group, based on resolution 26/4 of the Commission on Crime Prevention and Criminal Justice (UNODC/CCPCJ/EG.4/2018/CRP.1).

V. Adoption of the report

39. At its 6th meeting, on 5 April 2018, the Expert Group adopted its report (UNODC/CCPCJ/EG.4/2018/L.1).